ARMY CIO/G-6

Common Operating Environment

What is it?

The Common Operating Environment (COE) is an approved set of computing technologies and standards that enable secure and interoperable applications to be developed and deployed rapidly across five defined computing environments. Each computing environment has a minimum standard configuration that also supports the Army's ability to produce and deploy high-quality applications quickly while reducing the complexities of configuration, support and training associated with the computing environment.

Why is this important to the Army and to individual Soldiers?

Implementation of the COE will decrease the time it takes to deliver relevant applications to the warfighters who need them, and lower the cost of doing so.

What has the Army done?

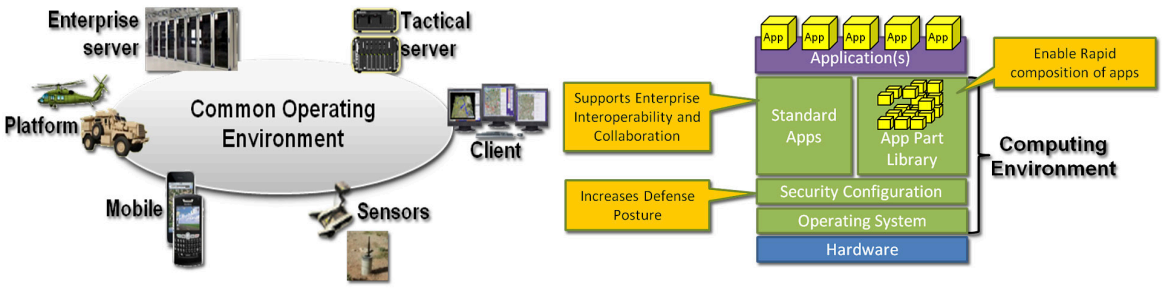
Army Software Transformation (AST) is a strategic initiative to alter the way the Army defines, develops, tests, certifies and delivers software applications to the Soldier. It sets three conditions necessary to developing and delivering software applications rapidly: standardized end-user environments (computing environments) and software development toolkits; a streamlined end-to-end enterprise software process; and creation of an Army Software Marketplace.

The COE addresses the first condition of AST. It applies a common operating environment to each of five categories of computing environments: servers (enterprise and tactical), platform (vehicles or aircraft), sensors, mobile/small form factor (PDAs) and client (desktop users). The computing environments, combined with a common architecture, will align the Army with industry best practices and, perhaps most importantly, enable the rapid development of secure and interoperable applications that satisfy operational requirements.

The COE also will help the Army execute information technology acquisition in a more efficient yet less expensive manner. For instance, the Army intends to pursue smaller programs, separating data from applications; and the use of common modules to accelerate software development.

What does the Army have planned for the future?

The next step is for the Assistant Secretary of the Army (Acquisition, Logistics and Technology) to develop the COE Implementation Plan, which will outline the steps and schedule for moving tactical Army systems to the COE. The intent is to: standardize end-user environments and software development kits; establish streamlined enterprise software processes that rely on common pre-certified, reusable software components; and develop deployment strategies that give users direct access to new capability. ■



An Enterprise Network: the Key to Army Transformation

The individual warfighter and the collective Army rely more heavily than ever before on information technology to execute the mission. To provide the data and capabilities Soldiers need, among them intelligence, surveillance, reconnaissance, communications and command and control, securely and on demand, the Army's network must become an enterprise system. Only by centralizing the network, known as LandWarNet, will the Army be able to make it sustainable, defensible and a truly operational capability.

The challenge is to deliver network services that are timely, relevant and focused on the warfighter via enterprise solutions that effectively and efficiently support the Army of the 21st century. Today's Army is a versatile mix of tailorable and networked organizations that operate on a rotational cycle and conduct wide-ranging full-spectrum operations. LandWarNet is the key to making this force structure successful, down to the tactical edge.

The Global Network Enterprise Construct (GNEC) is the Army-wide strategy for transforming LandWarNet into an enterprise network. The results, so far, are promising. Various exercises have successfully demonstrated that the enterprise concept is viable and achievable; procurement and construction of the physical network infrastructure are proceeding apace. ■

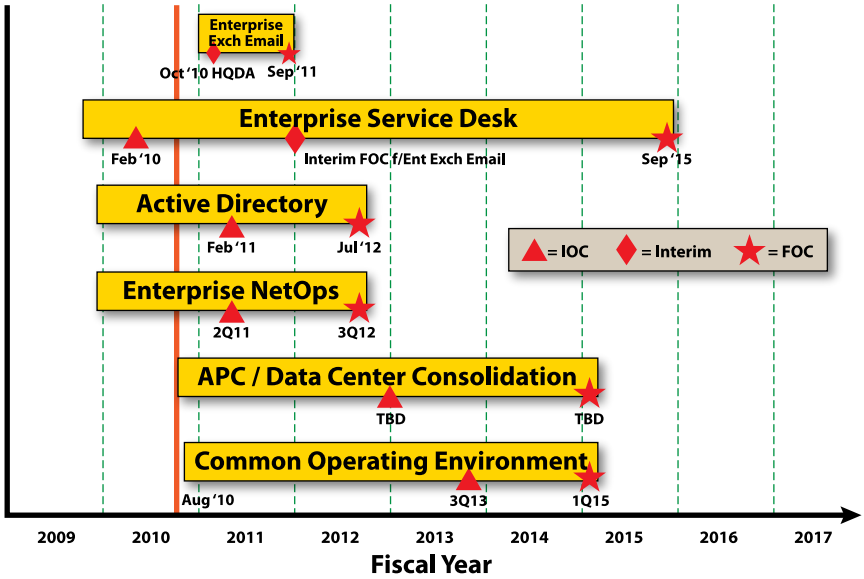
Why is LandWarNet transformation important to the Warfighter?

The ability to fight upon arrival is critical to enabling the predominantly CONUS-based Army to respond effectively to any threat in any environment. The Army's current networks, information systems and resources are not sufficient to support a true fight-upon-arrival capacity. Access to the network and information technology resources is inconsistent; units must deal with numerous IT-related changes as they move from one physical location to another and one phase of the Army Force Generation cycle to another. However, by providing all warfighters universal access to their applications, data and collaboration and training resources, as well as one email address and telephone number, the Army will achieve this essential fight-upon-arrival capability.

Where Are We Now?

In the past year, we have brought fidelity to the strategy, detailing plans for adopting industry standards and protocols, pursuing data center consolidation and establishing a common operating environment to accelerate software development and increase network security. Additionally, Army Cyber, a new command to oversee the operation and defense of Army networks, was activated. With fiscal reality and the always adapting enemy in mind, the Army will continue to define and refine network doctrine, tactics, techniques and procedures, and to incorporate technological advances, customer demands, national strategic objectives and process improvements into LandWarNet. ■

Top Strategic Initiatives and Implementation Timeline



Enterprise Exchange Email & Calendar

❖

Enterprise Service Desk

❖

Active Directory Migration

❖

Enterprise Network Operations (NetOps)

❖

Area Processing Center / Data Center Consolidation

❖

Common Operating Environment

Contact: CIOG6StratComm@conus.army.mil

U.S. ARMY